IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI WESTERN DIVISION

IN RE: T-MOBILE CUSTOMER DATA SECURITY BREACH LITIGATION,	)	MDL No. 3019
	)	Master Case No. 4:21-MD-03019-BCW
ALL ACTIONS	)	

ORDER DENYING PLAINTIFF ACHERMANN'S MOTION TO REMAND

Before the Court is Plaintiff James Achermann's Motion to Remand. (Doc. #133). The Court, being duly advised of the premises, having considered the motion, Class Counsel's opposition (Doc. #141), T-Mobile' opposition (Doc. #145), Achermann's replies (Docs. #146 & #159), and having heard oral argument on the motion during the final approval hearing, denies said motion.

Plaintiff Achermann argues he does not have Article III standing to pursue his action in federal court. (Doc. #133 at 7). Achermann seeks remand to pursue his claim in California state court on behalf of himself and the same California subclass that Plaintiffs in the MDL assert in the Consolidated Class Action Complaint ("Consolidated Complaint"). (Doc. #128). The claim Achermann seeks to litigate in California state court arises under the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code. §§ 1798.150, et seq is pleaded as Count 14 of the Consolidated Complaint.

In seeking a remand, Plaintiff Achermann argues that this Court lacks Article III jurisdiction over him, specifically due to the United States Supreme Court's recent opinion in TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021). However, Plaintiff Achermann himself, in his state court complaint (Doc. #133-1), has alleged facts sufficient to establish Article III standing. Moreover, the Consolidated Complaint in this MDL sets forth sufficient facts to establish standing on behalf of the class — which includes Achermann per his allegations that he was a part of the

T-Mobile Data Breach — such that the Motion to Remand on the basis of lack of standing must be denied.[1]

The Consolidated Complaint alleges that the sensitive PII of Plaintiffs' stolen by a hacker from T-Mobile was offered for sale on the dark web. (Doc. #128 ¶¶ 91-105). Achermann in his complaint similarly alleges that T-Mobile's Data Breach "subjected Plaintiff and the other Class Members to an unauthorized access and exfiltration, theft, or disclosure of their nonencrypted and nonredacted PII[.]" (Doc. #131-1). Because Plaintiffs have alleged that the proposed class members' (including Achermann's) PII was exfiltrated and posted on the dark web, he — like all other Plaintiffs in the MDL — necessarily has standing under TransUnion, wherein the United States Supreme Court held that the plaintiffs whose credit reports were wrongfully disclosed had standing based on that wrongful disclosure, regardless of whether any consequential harm flowed therefrom. TransUnion, 141 S. Ct. at 2204 (identifying that the "disclosure of private information" qualifies as a concrete injury for standing); see also In re American Medical Collection Agency, Inc. Customer Data Security Breach Litig., No. 19-md-2904, 2021 WL 5937742, at *8-9 (D.N.J. Dec. 16, 2021) (finding standing existed for plaintiffs who alleged their PII was for sale on the dark web and explaining that: "a plaintiff who suffers a wrongful disclosure need not additionally demonstrate misuse resulting in economic harm. For example, the named-plaintiffs in TransUnion did not allege direct economic harm beyond the dissemination of the misleading OFAC alert") (citing TransUnion, 141 S. Ct. at 2201)).

Moreover, the Plaintiffs in the Consolidated Complaint allege that they and the proposed Class "remain at a substantial and imminent risk of future harm" given the public disclosure of their data. (Doc. #128 ¶¶ 6-71, 91-94, 135-148). That the Plaintiffs are at "a substantial and

[1] As his counsel acknowledged at oral argument, Mr. Achermann could have opted-out of the pending class action settlement and pursued his claim individually in California state court as he wished.

imminent risk of future harm" is established by the fact that multiple Named Plaintiffs have suffered identity theft and fraud as a result of their PII being stolen in the T-Mobile Data Breach. (Doc. #128 ¶¶ 9, 10, 15, 18-19, 21-25, 27-30, 32-34, 38-40, 42, 44, 49-51, 53-55, 57, 59-61, 65-67, 69, 71). Because of the Data Breach, the Named Plaintiffs have taken mitigating actions resulting in concrete injuries, which include spending time and effort mitigating the risk of the breach, such as monitoring their accounts and freezing their credit. See, e.g., id. ¶¶ 6-71.

The harms alleged adequately show that Plaintiffs and the proposed class (including Achermann) have Article III standing, as numerous courts have held in the data breach context. See, e.g., Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 892 F.3d 613, 622 (4th Cir. 2018) (holding plaintiffs suffered injury in fact in a data breach case where they "suffered time lost in seeking to respond to fallout" from the data breach, had to "notify credit reporting agencies," and took other steps to "safeguard against future identity theft"); In re Zappos.com, Inc., 888 F.3d 1020, 1027 (9th Cir. 2018) (holding Article III standing established in a data breach case where the "sensitivity of the personal information, combined with its theft, led us to conclude that the plaintiffs had adequately alleged an injury in fact supporting standing"); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694-96 (7th Cir. 2015) (holding plaintiffs adequately alleged "imminent harm" given hackers had stolen their data and that "they have already lost time and money protecting themselves against future identity theft and fraudulent charges").[2]

[2] See also Anderson v. Hannaford Bros. Co., 659 F.3d 151, 164 (1st Cir. 2011) (mitigation efforts constituted compensable injury where the "deliberate taking of credit and debit card information by sophisticated thieves intending to use the information to their financial advantage" meant the victims "were not merely exposed to a hypothetical risk, but to a real risk of misuse"); In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 459 (D. Md. 2020) ("[G]iven the non-speculative nature of these alleged injuries, the plaintiffs' out-of-pocket costs and time spent to mitigate the harms also constituted injury-in-fact"); Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 749 (S.D.N.Y. 2017) ("[M]itigation expenses satisfy the injury requirements of negligence; otherwise Plaintiffs would face an untenable Catch–22" because "Plaintiffs were required to take reasonable steps to mitigate the consequences of the data breach").

Moreover, multiple courts have found Article III standing in similar data breach cases after TransUnion. See, e.g., In re: Blackbaud, Inc., Customer Data Breach Litig., MDL No. 2972, 2021 WL 2718439, at *6 n.15 (D.S.C. July 1, 2021) (explaining that TransUnion "would not impact the court's injury in fact analysis" given the TransUnion case had proceeded through a jury verdict whereas at the motion to dismiss stage the court must rely on the pleadings and was "not in a position to discern whether Plaintiffs 'factually establish[ed]'" concrete harm); In re Mednax Servs., Inc., Customer Data Sec. Breach Litig., No. 21-MD-02994-RAR, 2022 WL 1468057, at *7 (S.D. Fla. May 10, 2022) (finding that, given the theft of their PII, "in addition to establishing a substantial risk of future harm" Plaintiffs alleged "concrete harms sufficient to satisfy the Court's holding in *TransUnion*," including "the cost of the increased time Plaintiffs have spent and must continue to spend reviewing their financial information"); Clemens v. ExecuPharm Inc., 48 F.4th 146, 155-56 (3d Cir. 2022) (finding Article III standing in data breach case post-TransUnion and addressing TransUnion).

In seeking remand, Achermann relies heavily on In re SuperValu, Inc., 870 F.3d 763, 767 (8th Cir. 2017). But in that case, the Court's reasoning was based on the fact that the stolen payment card information "does not include any personally identifying information, such as social security numbers, birth dates, or driver's license numbers." Id. at 770. Plaintiffs' allegations here are decidedly different. Namely, in the Consolidated Complaint and as recounted above, Plaintiffs allege that their PII was stolen from T-Mobile — including their names, dates of birth, driver's license numbers, and Social Security numbers — and then listed for sale on the dark web. (Doc. #128 ¶¶ 91-95, 99-100). Plaintiffs' allegations here are therefore distinct from those in SuperValu — which has been distinguished by numerous courts in the Eighth Circuit for similar reasons. See, e.g., Mackey v. Belden, Inc., No. 4:21-CV-00149-JAR, 2021 WL 3363174, at *5 (E.D. Mo. Aug. 3, 2021) (holding that plaintiff who "had PII including her social security number stolen" had

standing, and distinguishing SuperValu, in which "the stolen data did 'not include any [PII], such as social security numbers'"); In re: Netgain Tech., LLC, Consumer Data Breach Litig., No. 21-CV-1210 (SRN/LIB), 2022 WL 1810606, at *5 (D. Minn. June 2, 2022) ("[T]he factual allegations here are different from the facts alleged in SuperValu," because in that case "the stolen card information did not include any PII," whereas "it is undisputed that the stolen Sensitive Information includes PII."); Weisenberger v. Ameritas Mut. Holding Co., 597 F. Supp. 3d 1351, 1359 (D. Neb. 2022) ("The kind of PII that the plaintiff alleged was compromised in the data breach — Social Security numbers, addresses, birth dates, names, addresses, and email addresses — is the kind of information, unlike mere credit card information, that can lead to a wide range of identity fraud."); Coffey v. OK Foods Inc., No. 2:21-CV-02200, 2022 WL 738072, at *3 (W.D. Ark. Mar. 10, 2022) ("Unlike in in re SuperValu," where "the stolen information was limited to credit and debit card information, here the amended complaint pleads stolen social security numbers which create a higher risk of identity theft.").

Because Plaintiffs have adequately alleged standing in their Consolidated Complaint and because Mr. Achermann himself has set forth allegations sufficient to establish standing in his own complaint, the Court finds that it has jurisdiction and the Motion to Remand is therefore denied. Accordingly, it is hereby

ORDERED Plaintiff James Achermann's Motion to Remand (Doc. #133) is DENIED.

DATED: June 28, 2023

/s/ Brian C. Wimes
JUDGE BRIAN C. WIMES
UNITED STATES DISTRICT COURT